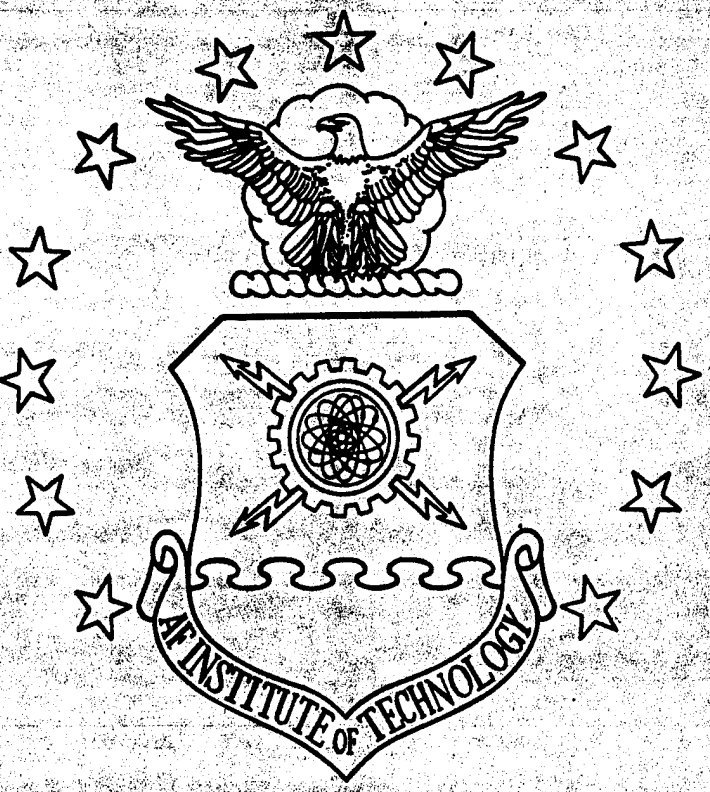

PLANNING FOR THE INFORMATION CAMPAIGN

Graduate Research Paper

Andrew H. Pears, B.S.
Captain, USAF

AFIT/GMO/LAR/96J-8

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GMO/LAR/96J-8

PLANNING FOR THE INFORMATION CAMPAIGN

Graduate Research Paper

Andrew H. Pears, B.S.
Captain, USAF

AFIT/GMO/LAR/96J-8

The views expressed in this graduate research paper are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

AFIT/GMO/LAR/96J-8

PLANNING FOR THE

INFORMATION CAMPAIGN

GRADUATE RESEARCH PAPER

Presented to the Faculty of the Graduate School of Logistics

and Acquisition Management of the Air Force Institute of Technology

Air University

In Partial Fulfillment of the

Requirement for the Degree of

Master of Air Mobility

Andrew H. Pears, B.S.

Captain, USAF

May 1996

Acknowledgments

I would like to thank my research advisor, Major Mike Shoukat, for his assistance throughout this research effort. He provided me with much needed guidance and direction. His assistance was invaluable. I would also like to thank Dr. Craig Brandt for his help in proofreading this paper and providing me many valuable comments.

This entire project would not have been possible without the support I received from my family. I would like to thank my wife Mary for her patience and encouragement throughout this entire process. I would like to thank my children, Joey, Jonathan, and Kayleigh, for their understanding when daddy was unable to attend some of their activities. Finally, I wish to thank my dog, Cassie, for sharing her dog biscuits with me when I came home late at night and missed supper.

Andrew H. Pears

Table of Contents

Page

List of Figures

List of Tables

Abstract

Desert Storm demonstrated the importance of dominating the information realm during a conflict. Information warfare is the means through which our forces can maintain information dominance on future battlefields. Air Force doctrine is currently being modified to include three new roles and missions related specifically to information warfare. Plans for future conflicts should include these new roles and missions.

Campaign plans serve as the unifying focus for our conduct of warfare. This study examines the various aspects of campaign planning and information warfare. This research provides future planners eight specific information campaign planning recommendations. It is recommended that the information campaign plan support the joint effort, follow the fundamentals of campaign plans (JCS Pub 5-0), and accomplish information warfare objectives. Furthermore, information campaign planners should examine communications network survivability, friendly and enemy centers of gravity, satellite systems capabilities and vulnerabilities, the possible effects of the media and specific user requirements.

PLANNING FOR THE INFORMATION CAMPAIGN

I. Problem Definition/Overview

Introduction

Operation Desert Storm officially started at 0300 local Riyadh time on 17 January 1991. It has been argued that this was also the start of the first information war. This operation produced many innovations that will affect how future conflicts are fought. One of the more important lessons we learned from Desert Storm was how large an impact information dominance can have on a conflict.

From the very first shots of Desert Storm, the allies targeted the Iraqi's information capability, degrading the enemy's capability to fight. The air campaign's initial objectives were designed to disable three critical information functions: the Iraqi integrated air-defense system, Saddam Hussein's command, control, and communications network, and the electric power generation and transmission systems that supported among other functions, Iraqi telecommunications (Winnefield, 1994:120-121). Through this targeting, planners hoped to disrupt Saddam Hussein's ability to communicate with both his military and civilian populations.

Computer viruses were introduced into American warfare for the first time during Operation Desert Storm. On 10 January 1992, ABC's Nightline reported that, according

to U.S. News and World Report, a computer virus was inserted into the Iraqi military computer system causing portions of the Iraqi defensive radar systems to be disabled (Schwartau, 1994:249). Though the truth of this report is not known, it can be confirmed that many of the allies' personal computers were shut down for hours and sometimes days by computer viruses attached to software programs deployed from the United States, or purchased on the local economy. Most units did not deploy with anti-virus programs.

Alan Campen wrote in his book, The First Information War, "By leveraging information, a much smaller and less expensive military force can continue to underpin U.S. foreign policy in an unpredictable and disorderly new world" (Campen, 1992:ix). Proper planning is essential to ensure information dominance in future conflicts. The three examples presented above show different perspectives of information warfare planning during the Gulf War. The air campaign's objectives depict an example of planning from an information warfare perspective, the introduction of a virus into an enemy's computer system represents potential information warfare planning area, and the lack of computer virus software shows the consequences of a lack of information warfare planning.

Description of the Problem

General Ronald R. Fogleman, Chief of Staff, United States Air Force (CSAF) discussed dimensions of warfare in a speech to the Armed Forces Communications and Electronics Association (AFCEA) in Washington, D.C. on 25 April 1995. In the speech, he discussed how up to the beginning of the 20th century war had been fought in two

dimensions, on a horizontal plane, land and sea. The development of the airplane added a vertical or third dimension that really came into its own during World War II. He went on to discuss how, in his opinion, space was the next major advancement in warfare, adding a fourth dimension. He then discussed a new dimension in warfare stating, "Information has an ascending and transcending influence -- for our society and our military forces. As such, I think it is appropriate to call information operations the fifth dimension of warfare. Dominating this information spectrum is going to be critical to military success in the future" (Fogleman, 1995:WWWeb).

Information warfare, including the information operations of gaining, exploiting, protecting and attacking information, is one of the hottest current topics at the Pentagon. (Widnell, 1995:WWWeb) There is an increasing amount of literature being written on the subject of information warfare in both the military and civilian sectors, but little of this literature is related to planning for information warfare activities. Information warfare needs to be incorporated into our planning processes. A campaign plan should be developed for information warfare just as these plans are developed for air warfare. The purpose of this paper is to identify considerations that need to be taken into account in the development of an information warfare campaign plan.

Need for Resolution

President George Bush signed National Security Decision Directive (NSDD) 145 on 5 July 1990. NSDD 145 established a national policy for the security of our telecommunications and information systems. Our national policy states:

> Telecommunications and information systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. (NSC, 1990:1)

Attacks on our telecommunications and information systems can have devastating effects. In November 1990, a backhoe operator accidentally severed a telephone line shutting down 150,000 telephones and O'Hare International Airport (Munro, 1995:WWWeb). Though this incident was purely accidental, attacks on our commercial telecommunications assets can be well planned to maximize the impact. At first, attacks on our nation's telecommunications systems may seem of little significance to our military forces, but when one considers that over 90 percent of our military communications occur over this commercial backbone, it quickly becomes evident how devastating such an attack could be on our ability to wage war (Kaplan, 1995:3). Plans need to be developed to protect our information systems and the information that resides on these systems, especially during time of conflict.

Our computer networks are also at risk to an information attack. Time magazine reported that, according to Pentagon officials, a group of Dutch hackers offered to disrupt our military's deployment during Desert Shield by infiltrating our computers. The cost of this attack was $1 million. Saddam Hussein turned down the offer (Waller, 1995:WWWeb). Robert Ayers, chief of the Defense Information Systems Agency's (DISA) information warfare division, put together a team of in-house computer experts to test the resilience of the Pentagon's computer networks against enemy hackers. The

results of this 1994 test showed hackers seized control of 88 percent of the 8,900 Pentagon computers they attacked and, probably even more disturbing, only 4 percent of these penetrations were ever detected (Munro, 1995:WWWeb).

The National Communications System, a DISA-managed unit responsible for assuring that a critical portion of our nation's information networks stays operational during any crisis, concluded in a December 1994 report, that no fewer than 30 nations are working on information warfare techniques (Munro, 1995:WWWeb).

Martin C. Libicki argues great change happens in two ways. In the first, a sleeper awakes in an entirely new world that is so different from custom it gives a sense of being in a foreign land. Although many of these changes are sudden and catastrophic, adjustment occurs in a conscious and often reactionary way. In the second, the sleeper awakes to a comfortable, easy world in which little seems changed. Eventually, some event occurs that causes the sleeper to look back and realize how far one has come so effortlessly. He argues that the challenge of information security is of the second type and this path is far more dangerous than the first (Libicki, 1994:1-3). If information warfare is a new dimension of warfare, and represents a change as great as the introduction of aircraft into warfare, it is crucial to understand the impact of this change so we do not follow the second path. We need to be prepared to defend against information attacks and exploit an enemy's information capabilities. An analysis of planning considerations will allow us to understand the information warfare environment and develop plans similar to those developed for air campaigns.

Our nation's military needs to keep a competitive edge on the information battlefield. As the examples above show, we are vulnerable to information warfare attacks in peacetime as well as wartime. More importantly, these attacks could occur as we are trying to transition from peacetime to war and severely hamper our deployment efforts. Many of our deployed information systems are extensions of fixed information systems. Corrupting a data base in the United States can degrade our warfighting ability just as much as targeting the system in theater. Plans need to consider information warfare on a global scale versus a theater only perspective, and be ready to be implemented as we transition from peacetime to wartime.

Identification of Problem Components

The investigative questions that form the foundation of this paper are:

1. What guidance does the Joint Chiefs of Staff provide for campaigns and campaign planning?
2. What are Warden's five rings model, and Boyd's observe, orient, decide attack (OODA) model and analyze how can these models be used in developing an information warfare campaign plan?
3. What is information warfare?
4. How can information warfare missions be used to accomplish information warfare objectives?
5. What should a planner consider in developing an information warfare campaign plan?

Plan of Attack

A common understanding of terms is critical to the discussion of any issue. First, campaigns and campaign planning will be discussed to give the reader a basic understanding of these concepts. Since campaigns are joint, a series of joint publications will be used to discuss campaigns, campaign planning and types of campaign plans.

Colonel Warden's five ring model and John Boyd's OODA loop model are commonly referred to in the information warfare literature. Campaign plans seek to defeat an enemy's centers of gravity while protecting friendly centers of gravity. The concept of center of gravity and how these models can be used to attack an enemy's center of gravity will be discussed. These models will be examined from the planner's perspective to analyze how they can be used in developing an information warfare campaign.

There is no universally accepted definition for information warfare. This paper will examine some of the different views on information and information warfare, and explain the perspective upon which the analysis will be based. Since this paper will be analyzed from the Air Force's view, the documents, Cornerstones of Information Warfare and Information Warfare Air Force Doctrine Document (AFDD) 5, Preliminary Draft, will be critical to the development of the information warfare concept.

Campaigns seek to achieve objectives. The analysis chapter of this paper will examine how Air Force information warfare missions can be used to achieve the Air Force's information warfare objectives. These missions will be explained and examples

of how these missions can be used to achieve information warfare objectives will be provided.

Finally, a list of considerations for information warfare campaign plans will be developed. These considerations will be discussed from the view point of developing a campaign plan. This list, while not all inclusive, will provide future information warfare planners a foundation for developing campaign plans.

II. Literature Review

Introduction

In this chapter, campaigns and campaign planning will be described. The documents that form the foundation of these descriptions are Joint Pubs 1.0, 3.0, and 5.0. Next, literature on two models of warfare will be reviewed and summarized. Different viewpoints on information and information warfare will then be discussed. Finally, the Air Force's basic guidance on information warfare will be presented.

Campaign Planning

A campaign is a series of related joint major operations that arrange tactical, operational, and strategic actions to accomplish strategic and operational objectives within a given time and space (JCS, 1995c:xiii). Campaigns represent the art of linking battles and engagements in an operational design to accomplish common objectives. They serve as the unifying focus for our conduct of joint warfare. Joint campaigns provide a common frame of reference within which land, sea, air, space, and information operations are integrated and harmonized (JCS, 1991:45).

A campaign plan describes how a series of joint major operations are arranged in time, space, and purpose to achieve a strategic objective. Through campaign plans, combatant commanders define objectives; describe concepts of operations and sustainment, arrange operations in time, space, and purpose; organize forces; establish

command relationships; assign tasks; and synchronize air, land, sea, space, and special operations, often in coordination with allies, interagency operations, non-government operations, and even United Nations operations (JCS, 1995b:III-7).

Joint Pub 5-0, Doctrine for Planning Joint Operations lists the following fundamentals of campaign plans:

- Provide broad strategic concepts of operation and sustainment for achieving multinational, national, and theater strategic objectives.
- Provide an orderly schedule of decisions.
- Achieve unity of effort with air land, sea, space and special operations forces, in conjunction with interagency multinational, nongovernmental, private voluntary, or United Nations forces, as required.
- Incorporate the combatant commander's strategic intent and operational focus.
- Identify any special forces or capabilities the enemy has in the area
- Identify the enemy strategic and operational centers of gravity and provide guidance for defeating them.
- Identify the friendly strategic and operational centers of gravity and provide guidance to subordinates for protecting them.
- Sequence a series of related major joint operations conducted simultaneously in depth.
- Establish the organization of subordinate forces and designate command relationships.
- Serve as the basis for subordinate planning and clearly define what constitutes success, including conflict termination objectives and potential posthostilities activities.
- Provide strategic direction; operational focus; and major tasks, objectives, and concepts to subordinates.

- Provide direction for the employment of nuclear weapons as required and authorized by the National Command Authorities. (JCS, 1995c:II-20)

Campaign plans form the basis for developing subordinate campaign plans and supporting plans. Subordinate campaign plans may be developed by subordinate Joint Forces Commanders (JFC) to accomplish or contribute to the accomplishment of theater strategic objectives. Subordinate unified commands typically develop these plans to accomplish assigned missions. Joint Task Force commanders may also develop subordinate campaign plans if missions require military operations of substantial size, complexity, and duration. Subordinate campaign plans should be consistent with the strategy, guidance, and direction developed by the combatant commander and should contribute to achieving combatant command objectives.

Supporting plans are prepared by subordinate and supporting commanders to satisfy the requirements of the supported commander's plan. Typically, supporting plans provide augmentation forces, force enhancements, or functional support, such as logistics, transportation, and communications (JCS, 1995b:III-20). The plan for the information campaign would be a supporting plan. This plan needs to support the overall campaign or subordinate campaign plan.

Two Models of Warfare

Two models are consistently mentioned in the literature on information warfare. Both these models, Warden's Five Rings Model and Boyd's OODA loop model focus on an enemy's commander, and influencing that commander's decision-making process.

Warden suggests attacking an enemy's centers of gravity, whereas Boyd suggests attacking the links that hold these centers of gravity together. These models could potentially be used in developing information warfare campaign plans.

Centers of gravity are the foundation of capability -- what Clausewitz calls "the hub of all power and movement, on which everything depends . . . the point at which all our energies should be directed." They are those characteristics, capabilities, or locations from which a military force derives its freedom of action, physical strength, or will to fight (JCS, 1995b:III-20).

Colonel John Warden's Five Rings Model. Colonel John Warden in his Airpower Journal article "The Enemy as a System," developed a model for use in warfare at the strategic and operational levels. Colonel Warden is credited for developing the initial plan for the Desert Storm air campaign, which was later refined and used to guide allied air efforts. His book, The Air Campaign, deals with air power theory and practice at the operational level.

Colonel Warden's model consists of five concentric rings. Each of these rings describes a set of critical targets. The five rings model is shown in Figure 1 (Warden, 1995:47).

The command or leadership ring is at the center of Warden's model. This ring represents the enemy command structure and could be the civilian or military head of government or a military commander. In the strategic model, this command element is the only element that can direct the nation at war, make concessions, and make complex

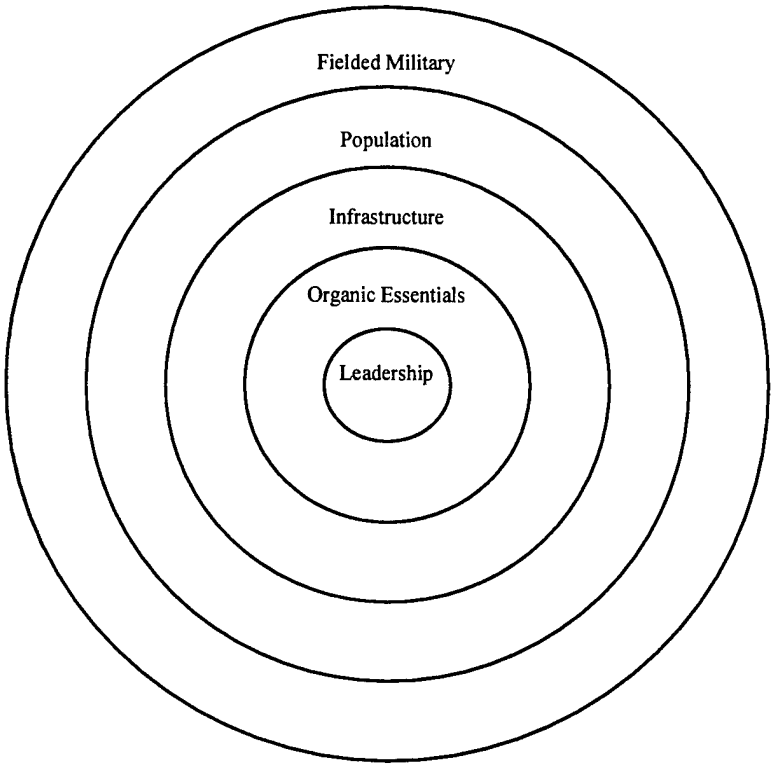

Figure 1. The Basic Five-Ring Model

decisions required to keep a nation on a particular course. Since capturing or killing a state's leader is very difficult to do, command communications can be targeted making it difficult for the leader to direct war efforts or maintain the support of the state's populous. Even when the commander cannot be directly threatened, other centers of gravity can be carefully selected to exert indirect pressure on the commander with the objective of forcing him to concede to our will (Warden, 1995:49-50).

The second most important ring in this model is organic essentials. Organic essentials are "those facilities or processes without which the state or organization cannot maintain itself (Warden, 1995:50). Organic essentials are dependent on the state or organization but can include products such as electricity, petroleum products, and food.

These essentials may not be directly related to combat, but may relate to the civilian population. The nation's population may in turn force the leader to make concessions because the political repercussions are too costly for the leader to bear. The attacks on organic essentials could make it difficult or impossible for the state to wage war or continue a particular course.

The next ring, infrastructure, contains the enemy's transportation system and the majority of a state's industry. All industry not in the organic essential ring would fall in the infrastructure category. Transportation targets would include the state's roadways, bridges, railways, airfields, airways, and seaports. This infrastructure is required to transport goods, services, and information inter-state and intra-state for both civilian and military purposes. "If this movement becomes impossible, the state system quickly moves to a lower energy level, and thus to a lesser ability to resist the demands of its enemy" (Warden, 1995:50). Since there are more targets and greater redundancy built into the infrastructure, a larger effort is required to do enough damage to have an effect on the enemy (Warden, 1995:50).

The fourth ring is the state's population. Due to moral reasons and the large number of targets involved, this ring is difficult to attack directly. However, Warden states, "indirect attack on the population . . . may be especially specially effective if the target country has a relatively low interest in the outcome of the war" (Warden, 1995:50).

The last ring is a state's fielded military forces. The only purpose of these fielded forces is to protect the state's inner four rings, or attack the rings of an enemy. Reducing a state's military forces can lead to concessions, because the other four rings are left unprotected. Though traditionally thought of as the primary target in warfare, the fielded troops are a "means to an end" (Warden, 1995:51).

Warden states, "The essence of war is applying pressure against the enemy's innermost strategic ring -- its command structure" (Warden, 1995:52). An attack on the other rings is not conducted for the effect on an enemy's fielded forces, but rather for the effect on the national leaders and commanders or on the enemy system as a whole. Though we have looked at the five rings model from a strategic perspective, the model can be applied at the operational level, with the operational and strategic targets summarized in the Table 1 (Warden, 1995:44-54).

Table 1. Targeting Enemy Systems

Level of Warfare	**Strategic**	**Operational**
Targeted System	State • communications • security	Enemy's fielded military forces • communications • security
Leadership	Government	Operational-level commander
Organic Essentials	Energy (electricity, oil, food) and money	Logistics (ammunition, fuel, food)
Infrastructure	Transportation system, majority of state's industry	Roads, airways, seaways, communications lines
Population	People	Support personnel
Fighting Mechanism	Fielded forces	Fielded forces

Colonel John Boyd's Orient, Observe, Decide, Act (OODA) Loop Model.

Colonel Boyd's concepts may at first seem diametrically opposed to those of Colonel Warden. Boyd views the cognitive process as the key to prevailing in a highly unpredictable and competitive world. Through his analysis of the fields of mathematical logic, physics, and thermodynamics, Boyd theorizes the following: "One cannot determine the nature of a system within itself and, furthermore any attempts to do so will lead to greater disorder and confusion" (Fadok, 1995:14). Boyd felt instead that victory in conflict war was a result of successfully forcing an inward orientation on the enemy by folding him back inside himself.

The military objective according to Boyd is "to break the spirit and will of the enemy command by creating surprising and dangerous operational and strategic situations" (Fadok, 1995:14). Due to the uncertainties of war, this can be done by denying the enemy the time needed to mentally handle difficult situations. Military operations attempt to deny the enemy time by:

1) Creating and perpetuating a highly fluid and menacing state of affairs for the enemy.
2) Disrupting or incapacitating the enemy's ability to adapt to such an environment (Fadok, 1995:14).

Boyd's four key qualities of successful military operations are initiative, harmony, variety, and rapidity. He feels these characteristics can be used to adapt and shape the wartime environment. To increase adaptability in wartime, one must minimize friction. On the other hand, a conflict can be shaped in one's favor by creating and exploiting the

frictions faced by one enemy. The goal becomes to minimize one's own friction while maximizing that of the enemy.

Initiative and harmony are the keys to minimizing friendly friction. Friendly friction is minimized by acting and reacting more quickly than the enemy. Initiative allows for personnel at the lower levels freedom of action. These personnel can determine how things are done. Harmony ensures all forces are working together for a common vision and is concerned with what gets done and why it is done (Fadok, 1995:15).

The keys to maximizing an enemy's friction are variety and rapidity. The object is to attack the enemy with a wide variety of actions as quickly as possible. These actions will reduce the enemy's capability to identify and react to those actions that are most threatening. One attempts to present an enemy rapidly and repeatedly with a combination of events that are ambiguous and deceptive, but threatening. The enemy will no longer be able to distinguish between those events that threaten their survival and those that do not. "In consequence, he can no longer determine what is being done to him and how he should respond. . . . By steadily reducing an opponent's physical and mental capabilities to resist, one ultimately crushes his moral will to resist as well" (Fadok, 1995:15).

Boyd advocates penetrating an enemy's "moral-mental-physical being to dissolve his moral fiber, disorient his mental images, disrupt his operations, and overload his system" (Fadok, 1995:15). Rather than attacking the enemy's centers of gravity as

proposed by Warden, Boyd proposes creating non-cooperative centers of gravity by attacking these moral-mental-physical linkages that bind the centers of gravity together. This should result in destruction of an enemy's internal harmony and external connection to the real world (Fadok, 1995:15).

Boyd's OODA model is derived from his contention that all rational human behavior, organizational or individual, can be depicted as a cycle of the four distinct tasks of observation, orientation, decision and action. The OODA loop is shown below (DAF, 95b:2)

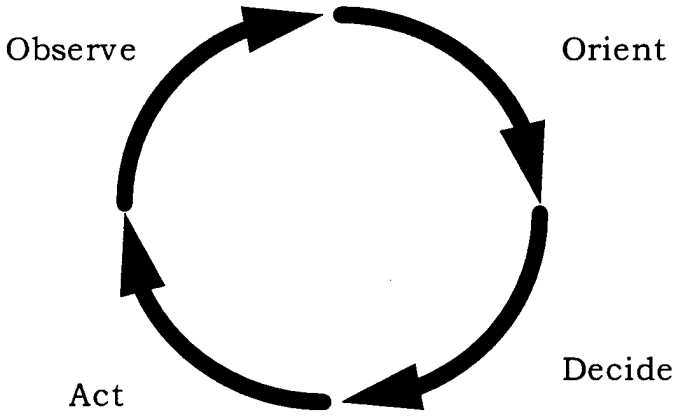

Figure 2. The OODA Model

The model states that the winner of a conflict will be the one who consistently moves through the OODA loop more accurately and rapidly than the enemy. Boyd contends that efficient and effective orientation is the main factor in loop speed and accuracy. One's

ability to orient and reorient will affect the accuracy and timeliness of decisions made in an uncertain wartime environment. One's own loop can be minimized by reducing friction through initiative and harmony of response. An enemy's loop can be maximized by increasing friction through variety and rapidity of response (Fadok, 1995:16-17).

The OODA loop can be looked at from the perspective of the traditional rational-choice decision making model. This model views decisions as the product of conscious decisions (Schwenk, 1988:13). The observation portion allows one to identify the problem. Identifying alternatives would be part of the observation and orientation processes. Evaluating alternatives would allow one to orient oneself. The decision phase would be where one selects an alternative. Implementing the alternative would be the act phase.

The traditional rational-choice model assumes one has all the possible information about the situation and complete knowledge of the consequences that will follow from all possible alternatives. This allows one to make the best solution. This is rarely, if ever, the case in wartime. H.A. Simon developed the concept of satisficing, where one selects the first solution that satisfies resolution of the problem versus the best solution (Schwenk, 1988:17). Attacking the enemy's observe and orient loops can cause an enemy to satisfice for a poorer quality decision, due to the lack of information about the problem, and consequences of potential alternatives.

What is Information?

Colonel Richard Szafranski in his Airpower Journal article, "A Theory of Information Warfare Preparing for 2020", prefers to uses Chris Mader's definition for information from the book Information Systems: Technology, Economics, Applications. Mader defines information as the "content or meaning of a message" (Szafranski, 1995:57). Szafranski goes on to define information systems as "a comprehensive set of the knowledge, beliefs, and the decision-making processes and systems of the adversary" (Szafranski, 1995:57).

Arquilla and Ronfeldt state in their seminal work on control warfare that information is more than the content or meaning of a message. They define information as "any difference that makes a difference" (Arquilla and Ronfeldt, 1993:WWWeb). This allows for the inclusion of messages where the message may be encrypted or meaningless to the receiver. There is still information value in this message due to the fact that communications occurred (Magsig, 1995:WWWeb).

Arquilla and Ronfeldt offer another view on information in their article, Cyberwar is Coming!. In this article, the authors point out that information is a difficult term to define, and defining it remains a key problem of the information revolution. They viewed information as a hierarchy with data at the bottom, information in the middle, and knowledge at the top. Arquilla and Ronfeldt acknowledged that they used the term information to mean something more than data but less than knowledge (Arquilla and Ronfeldt, 1993:WWWeb).

Another aspect of information of special relevance to the military is related to the information theory research conducted by Claude Shannon in 1948. Shannon's Law basically states that lower probability events contain more information than higher probability events. Using an example related to the military, there is probably more information in the fact that 200 pizzas are delivered to the Pentagon at nine o'clock in the evening than if 20 pizzas are delivered at lunch time. The former would probably tend to alert the news media to start watching military affairs more than the latter (Magsig, 1995:WWWeb).

Cornerstones of Information Warfare, the Air Force's basic guidance for information warfare, views information as being derived from phenomena, where phenomena are observable facts and events and include everything that happens around us. To become information, these phenomena must be first perceived (observed) and then interpreted (analyzed). Information is viewed as the result of two things: our perceptions of the phenomena (data) and the instructions required to interpret and give meaning to this data. Since information is dependent only on data and instructions, information is distinct from technology. Technology determines what we can do with the information and how fast we can do it.

The term information function is used to incorporate technology-dependent elements into information (DAF, 1995a:2-3). Information function is defined as "any activity involving the acquisition, transmission, storage, or transformation of information" (DAF, 1995a:3). It is understood that there are military information

functions that are different from the complete set of information functions. The term military information function is used to describe information functions that are force enhancing. Military information functions are defined as "any information function supporting and enhancing the employment of military forces" (DAF, 1995a:3).

Information Warfare Defined

Information warfare has been defined different ways over the past few years. Winn Schwartau, in his book Information Warfare Chaos on the Electronic Superhighway, defines information warfare as:

> An electronic conflict in which information is a strategic asset worthy of conquest or destruction. (Schwartau, 1994:13)

This definition is probably the best known in the civilian sector. Schwartau furthermore defines three classes of information warfare; personal, corporate, and global.

Personal information warfare is waged against an individual. It includes accessing digital records and database entries of individuals. This type of warfare can be executed against our military personnel. A friend of mine recently had over $2000 dollars withdrawn from automated teller machines through the use of his stolen credit card. The perpetrator of this crime used his military records to obtain his social security number and then used this to change his personal identification number with the credit card company. This example shows the need for protection of personal information by our military.

Schwartau identifies corporate information warfare as the second class. This class is concerned with the competition for information between corporations around the world. This type of warfare can involve stealing corporate secrets, destroying information in a corporation's data base or spreading information, real or fictitious, about a competitor or their products. This class of information warfare is also of significance to the Department of Defense. It could involve allies accessing our computer systems to obtain sensitive information, malicious hackers shutting down our electronic systems, or organizations launching a disinformation campaign against our military to sway public opinion.

The third class of warfare, global information warfare, is also the most damaging. This category of information warfare is concerned with the ability of an adversary to wage war against nation-states and political or economic spheres of influence. Class three warfare enables information attacks over thousands of miles (Schwartau, 1994: 19). This type of information warfare, due to the global nature, is of greatest concern to our military forces.

Emmet Paige, the Assistant Secretary of Defense for Command, Control, Communications, and Computers developed the Department of Defense definition for information warfare. This definition states information warfare is:

> Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and systems. (Haeni, 1995:WWWeb)

This definition considers only the strategic military aspect of information warfare. It also points out that information warfare supports our national military strategy. It does not consider how information warfare can affect individuals and organizations in ways not related to national security (Magsig, 1995:WWWeb). Also, information warfare can be offensive, affecting adversary information and information systems, or defensive, defending our own information and systems.

In 1995, the Air Force published the document Cornerstones of Information Warfare. This document provides the basic guidance for information warfare in the Air Force. In this document, information warfare is defined as:

> Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions. (DAF, 1995a:3-4)

This definition is the basis for the following assertions (DAF, 1995a:3-4):

1. Information warfare is any attack against an information function regardless of the means.

2. Information warfare is any function to protect our information functions regardless of the means.

3. Information warfare is a means, not an end, in precisely the same manner that air warfare is a means, not an end.

The Air Force goal of information warfare is information dominance. Information dominance is "that degree of superiority in information functions that permit friendly

forces to operate at a given time and place without prohibitive interference by the opposing force" (DAF, 1995b:1).

The Air Force doctrine currently recognizes air and space warfare. There is currently, in draft form, an Air Force Doctrine Directive that will incorporate information warfare into our doctrine. Just as there are three objectives for air warfare, there will be three information warfare objectives. The three proposed objectives are:

1. Control the information realm so we can exploit it while protecting our own military information functions from our enemies.
2. Exploit control of information to employ information warfare against the enemy.
3. Enhance overall force effectiveness by fully developing military information functions (DAF, 1995:8-9).

III. Analysis

Introduction

Currently, Air Force doctrine recognizes air and space warfare. Cornerstones of Information Warfare proposes changes to Air Force doctrine to add new roles and missions for information warfare just as there are for air and space. The new proposed role and missions are shown in italics in the table below (DAF, 1995a:8, 11).

Table 2. Roles and Missions of Aerospace Power

Aerospace Control	**Force Application**	**Force Enhancement**	**Force Support**
	Strategic Attack	Airlift	Base Ops & Def
Counterspace	Interdiction	Air Refueling	Logistics
Counterair	Close Air Support	Spacelift	Combat Support
Counterinformation	*C2 Attack*	Special Operations	On Orbit Support
		Information Operations	

In this chapter, these proposed new roles and missions will be analyzed as to how they can be used to meet the objectives of information warfare. As will be shown, the U.S. military already performs these missions to some extent. The focus of this analysis will be as to how these missions can be used to achieve the objectives of information warfare. The use of centers of gravity for targeting in the information campaign will also be discussed.

Controlling the Information Realm

The first objective the information campaign needs to satisfy is controlling the information realm. Our forces need to exploit the enemy's information realm while protecting our own military functions from enemy action. Counter information is a new Air Force mission consisting of actions dedicated to controlling the information realm. Combined with the current missions of counter air and counter space, counter information creates an environment where friendly forces can conduct operations without suffering substantial losses, while simultaneously denying the adversary the ability to conduct those operations against friendly forces. Counter information can confuse, delay, or inhibit enemy offensive actions and reduce reaction time for critical defensive measures. Counter information can be offensive or defensive. (DAF, 1995:8-9)

Defensive Counter Information. Defensive counter information includes both active and passive actions to protect ourselves from the enemy's information warfare actions. Defensive counter information is accomplished through actions such as physical defense, physical security, hardening, COMSEC, OPSEC, COMPUSEC, and counterintelligence. These actions can be used to assess the threat and reduce friendly vulnerabilities to an acceptable level. (DAF, 1995a:9)

One way a campaign planner can use defensive counter information is to design communications networks that are as invulnerable as possible to the destruction of individual stations and the links connecting these stations. Graph theory provides some useful tools for designing such a network. A communications network can be drawn as a

graph where the nodes represent ground terminals such as communications switches or satellite terminals and the edges represent the communications medium that connects these switches.

The graph below represents a communications network with 8 ground stations (nodes) and 16 links (edges).

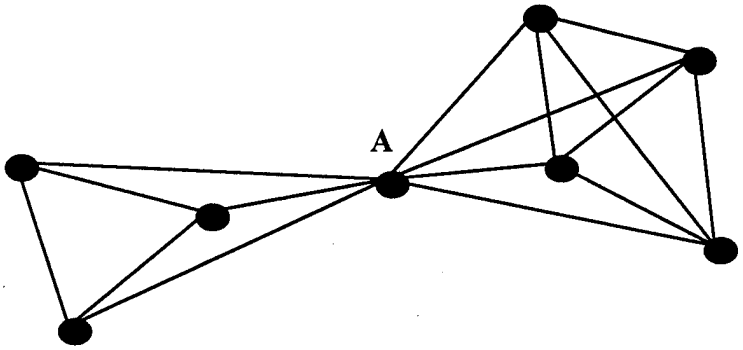

Figure 3. Separable Graph with 8 Nodes and 16 Edges

The edge connectivity of a graph can be defined as the minimum number of edges that when removed disconnect the graph. A graph is connected if there is at least one path between every pair of nodes. Otherwise, the graph is disconnected. The edge connectivity of this graph is three. The removal of the three edges to the left of node A will result in a disconnected graph. This is the minimum number of edges that when removed result in the graph being disconnected. These three links would have to be disrupted, possibly by jamming, to separate the communications network.

The node connectivity is defined as the minimum number of nodes whose removal leaves the graph disconnected. The node connectivity of the above graph is one. The removal of node A will disconnect the graph. By definition, a graph whose node connectivity is one is called a separable graph. The destruction of the communications ground station at A will result in a disrupted communications flow for the network (Deo, 1974:21, 75-78). There is probably a better way to design this network.

The graph below is another way to configure a communications network with 8 ground stations and 16 links.

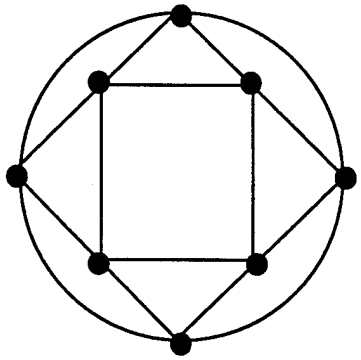

Figure 4. Graph with 8 Nodes and 16 Edges

The edge and node connectivity of this graph are four. Therefore, four ground stations would have to be destroyed or four communications links jammed to disconnect this network design. This network is less vulnerable to destruction than the previous network. A greater amount of an enemy's resources would be required to destroy this communications network. The campaign planner should use the second network design.

The question becomes what is the highest node and edge connectivity that can be achieved given the number of ground stations (n) and the number of communications links (e). Deo provides two theorems concerning the determination of node connectivity. Theorem 1 states that the node connectivity of any graph can never exceed the edge connectivity. Theorem 2 states that the maximum node connectivity one can achieve with a graph of n nodes and e edges, where $e \geq n-1$, is the integral part of the number $2e/n$, or $\lfloor 2e/n \rfloor$ (Deo, 1974:77-78). Theorems 1 and 2 can be summarized as follows:

$$\text{node connectivity} \leq \text{edge connectivity} \leq \lfloor 2e/n \rfloor$$

Thus, for a graph with 8 nodes and 16 edges, we can achieve a vertex connectivity, and therefore edge connectivity, as high as 4.

Preparations for Jamming. A campaign planner must be prepared to deal with enemy jamming. How effective will our communications be under conditions of enemy jamming? Satellite communications offers us the most capacity for supporting information flow, but is also highly susceptible to jamming. It would be difficult for a country to employ full-time barrage jamming across all frequencies or even the frequencies of UHF, C-band and X-band used by satellite communications. Besides needing an incredible amount of power to maintain barrage jamming, our enemies should expect to be attacked and destroyed if any of our frequencies are jammed for long, continuous periods of time. Therefore, the realistic goal of an enemy jammer is to reduce the ability to communicate not to completely disrupt it. We can probably expect sporadic

jamming of our key command, control links during the most critical times, probably right after we or the enemy has launched some type of offensive.

Unfortunately, the majority of military satellite terminals and all commercial satellite terminals have little or no jam resistance. The TSC-94A and TSC-100A are the USAF's only terminals offering a degree of jam resistance, but not without degrading the communications system. The anti-jam mode of operation is characterized by an extremely significant reduction in available capacity to assure communications capability to high priority users (Spellman, 1985:111).

The planner will have to examine the enemy's electronic order of battle. Questions will need to be asked such as how long the enemy would try to jam our communications satellites both consecutively and during a period of time (24 hours). Also, if both our military and our enemy's civilian population are using INTELSAT for commercial telephone service, can we expect the enemy to jam this asset? Plans to deal with enemy jamming and how to allocate reduced satellite capacity should be included in the campaign plan.

The Iraqis made no attempts to jam or disrupt our satellite communications. In fact, the only significant interference encountered was self-interference (Bedrosian and others, 1991:2). But the potential effects of enemy jamming on our communications systems cannot be discounted. Future potential enemies may be much more capable than the Iraqis.

Offensive Counter Information. While planning for defensive operations is an important aspect of campaign planning, offensive operations usually win wars. Offensive counter information allows friendly forces to use the information realm while disabling the enemy's use of information operations. (DAF, 1995a,9) Typical offensive actions we can use in the information campaign include: physical attack, military deception, psychological operations, electronic warfare, and information attack.

During Operation Desert Storm, the coalition forces were able to greatly compress their OODA loop with respect to Iraq's. The coalition forces had a much better ability to observe correct inputs, allowing reduced time to orient, decide and eventually act. The two loops are shown in Figure 5. The larger loop represents a longer amount of time to complete the OODA cycle.

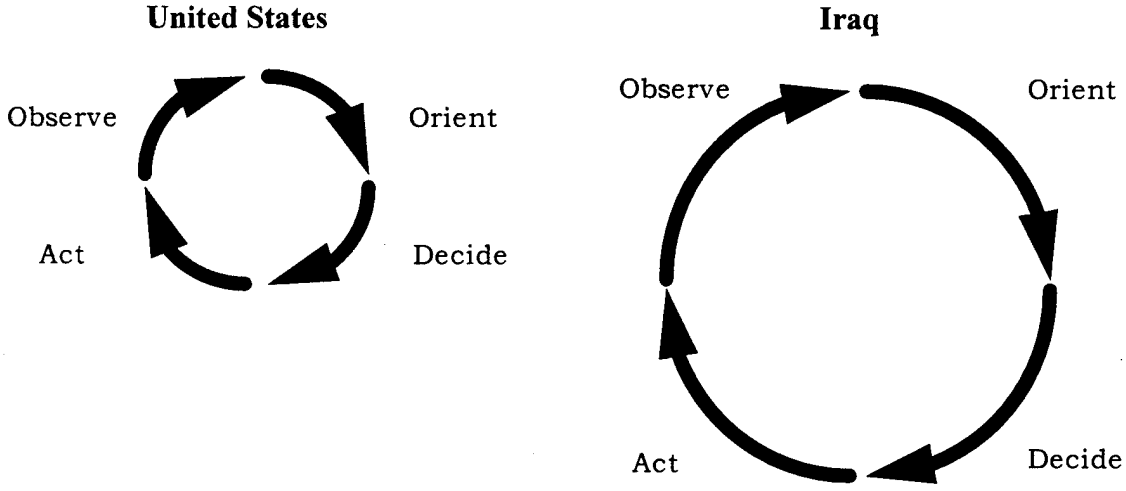

Figure 5. Expanded OODA Loop

Military deception and psychological operations are offensive actions that can be taken to expand an enemy's OODA loop.

Military psychological operations are planned to convey selected information and indicators to an enemy to influence their emotions, motives, objective reasoning, and ultimately their behavior (JCS, 1993:I-1). Psychological operations use information to affect the enemy's reasoning (DAF, 1995b: 5). Psychological operations can expand an enemy's OODA loop by affecting an enemy's reasoning.

Psychological operations can use the truth to demoralize the adversary, and thereby reduce their capability to respond to our actions. During Desert Storm, leaflets were dropped over Iraqi troop concentrations. These leaflets announced when a particular Iraqi ground unit was to be bombed. The unit was bombed the next day. This announcement and bombing cycle was then repeated (Cohen, 1993:339).

During Desert Storm, over 29 million leaflets were dropped in theater. Aerial PSYOP platforms averaged 19.5 hours per day of broadcasting. Radio PSYOP transmission averaged 17 hours per day. It is estimated that over 73,000 Iraqis were exposed to these efforts. The following table shows the exposure and effectiveness percentages for psychological operations conducted during Desert Storm.

Table 3. PSYOP Exposure and Effectiveness Percentages

	Leaflets	Radio	Loudspeakers
% Exposed to PSYOP	98	58	34
% Believed PSYOP Msg	88	46	18
% Influenced to act	70	34	16

These percentages are based on interviews by the 13th PSYOP Battalion on Iraqi prisoners of war (POW) (Cohen, 1993:336).

Boyd states that an enemy's OODA loop can be expanded by creating dangerous situations. The enemy will become disoriented and not have the necessary time to react to these situations (Fadok,1995: 14). The fact that 70 percent of the Iraqi POWs were influenced to act based on the leaflets would seem to give some credibility to the use of this technique in future conflicts. Future information planners need to incorporate psychological operations into their campaign plans.

Military deception is defined as being those actions executed to deliberately mislead adversary decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the enemy to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JCS, 1994:I-1). Military deception misleads the enemy about our capabilities and intentions (DAF, 1995a:5). Military deception can expand an enemy's OODA loop by giving the enemy false observations making it more difficult for the enemy to orient.

Central Command's (CENTCOM) Desert Storm deception plan had four main goals:

1) Mislead the Iraqi military staff as to CENTCOM's force composition, intentions, capabilities, and timing.

2) Encourage Iraq to misallocate resources moving into Kuwait.

3) Achieve and maintain a tactical advantage during the battle.

4) Minimize attrition of friendly forces.

Central Command Air Forces (CENTAF) then developed a deception plan to support CENTCOM's goals. CENTAF's supporting deception operations were designed to:

1) Condition Iraqi commanders to conclude that Coalition forces believed Kuwait to be the center of gravity.

2) Condition Allied air forces to fly a tempo of operations similar to what Iraq would see on the night of the real attack.

3) Develop a plan for masking the launch and movement of mission aircraft (air refuelers, etc.)

4) Exploit situations where repeated tactics created conditioned responses

5) Shut down Iraqi reconnaissance assets, thereby allowing coalition ground forces to move unobserved. (Cohen, 1993:319)

CENTAF's training scenarios were developed to allow Iraq to see Kuwait as the center of gravity. CENTAF positioned air refueling tracks in northeastern Saudi Arabia to allow Iraqi electronic intelligence to see them. The western tracks were placed outside of Iraqi radar coverage (Cohen, 1993:319).

During Desert Shield, training exercises conditioned the Iraqis to a standard air picture. The Iraqi radar operator became accustomed to seeing tankers, AWACS, Rivet Joint, and combat air patrols flying predictable patterns in the general vicinity of the

border. The plan included surges once a week. The surge on the first night of the war was eventually aligned with this schedule (Cohen, 1993:172, 326).

CENTAF's deception operations conditioned the enemy to seeing large numbers of aircraft in the air at regular intervals. When the first attack was launched, the Iraqis probably initially thought it was just another training exercise. Deception operations caused a delay in the enemy's ability to orient themselves to the situation.

Military deception is another area that needs to be addressed in the information campaign plan. This plan needs to support the broad goals set out in the combatant commander's deception plan. Deception is another way we can leverage information to control the information realm.

Physical attack, electronic warfare, and information attack can be used to disrupt an enemy's OODA loop. During Operation Desert Storm, we were also able to disrupt Iraq's OODA loop, as shown below. Disrupting the OODA loop eliminates a portion of this cycle stopping the flow of information versus increasing the amount of time it takes to flow through the cycle. This disruption degrades the enemy's capability to adapt to the combat environment. Figure 6 shows a disrupted OODA loop.

Physical attack can perform information warfare by affecting information systems through the conversion of stored energy to destructive power. The means of physical attack range from conventional weapons to electromagnetic pulse weapons (DAF, 1995a:5).

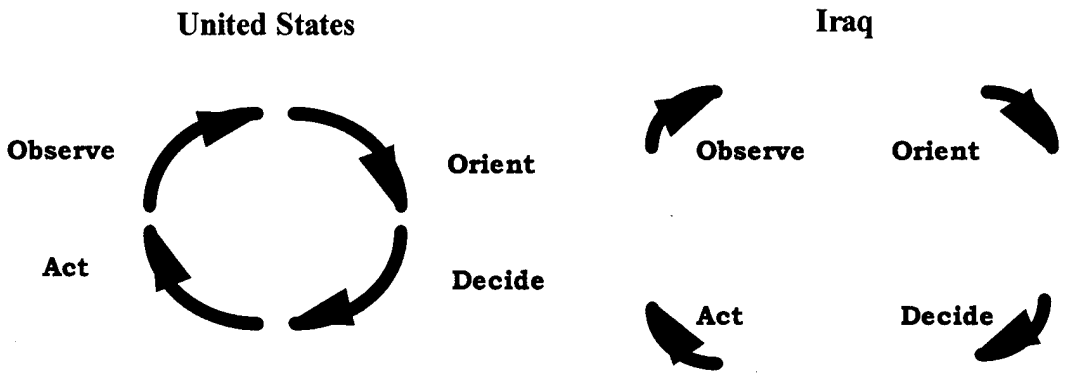

Figure 6. Disrupted OODA Loop

Electronic warfare is any military action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack an adversary. Electronic warfare denies accurate information to the enemy (DAF, 1995a:5).

The suppression of Iraq's air defenses provides an example of how physical attack can be used in concert with electronic warfare during the information campaign. On the first night, more than 200 High-Speed Anti-Radiation Missiles (HARM) were fired at Iraqi radar sites. These HARMs carried out a physical attack role. Meanwhile, aircraft jammed (electronic warfare) many of the remaining radar sites (Winnefield, 1994:121-22). Eliminating Iraq's radar capability essentially disrupted the observe portion of Boyd's OODA loop.

Information attack encompasses special communications and computer activities taken to manipulate or destroy an adversary's information functions. Information attack is directly corrupting an enemy's information without visibly changing the physical entity within which it resides (DAF, 1995a:6). Penetration of an enemy's information systems

has great value in combat. Manipulation of data bases or parameters of reporting systems can cause incorrect information for decisionmaking or destroy the enemy's confidence in their system (DAF, 1995a:5).

Exploiting Control of Information

The information campaign plan must satisfy the objective of exploiting the control of information to employ information warfare against the enemy. Information warfare can be used to conduct or support the traditional Air Force missions that exploit air control; strategic attack, interdiction, and close air support. In addition, the Air Force has added a new mission, command and control (C2) attack.

C2 Attack. C2 attack seeks to disrupt and destroy an enemy's C2. C2 is defined as the exercise of authority and direction over forces. The more dependent an enemy's C2 is on information and information systems, the more vulnerable C2 will be to attack. Effective use of C2 attack allows commanders to shape operations by controlling an adversary's ability to correctly assess situations and take appropriate actions (DAF, 1995b:8).

The question becomes how does the information campaign planner target C2. Warden suggests using centers of gravity, "that point where the enemy is most vulnerable and the point where an attack will have the best chance of being decisive," as a central theme in planning war operations. Then, the commander, has as his most important

responsibility, the responsibility to identify correctly and strike appropriately these enemy centers of gravity (Warden, 1988:9-10).

Warden does provide basic guidance on center of gravity identification stating, "Command is a true center of gravity and worth attack in any circumstance in which it can be reached" (Warden, 1988:53). The three elements or spheres of command are information gathering, decision, and communication. They can be attacked directly or indirectly, individually or together as a group. Disabling an enemy's radar systems, intelligence sensors, or early warning aircraft are examples of attacks on the information gathering element of command. The decision element, though essential, is usually the most difficult to attack directly. These attacks can range from directly targeting the command element's headquarters, to developing a deception plan that induces the commander to make a poor decision. The communications element can be disrupted with direct attacks on a nation's telecommunications exchanges, or possibly with attacks on electric power generation and transmission systems. Since the decision element is usually less vulnerable to attack, information gathering and communications are the elements to be targeted. These attacks can render a commander ineffective by isolating him from his forces and sources of information (Warden, 1988:53-57).

Enhancing Overall Effectiveness

The information campaign needs to support the overall objective of enhancing overall effectiveness by fully developing military information functions. The Air Force has developed a new mission, information operations, to accomplish this objective.

Information operations are defined as, "any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces" (DAF, 1995a:11).

Satellite Communications During Operation Desert Shield/Storm. Satellite communications is a key information function for enhancing the effectiveness of our forces. The Gulf War highlighted our dependence on satellite communications. Lieutenant General James S. Cassity, then J-6 of the Joint Staff, commented, "The services put more electronics communications capability into the Gulf in 90 days than we put in Europe in 40 years." Communications satellites provided over 95 percent of the communications into and out of the theater, and was used extensively to support intra-theater requirements across long distances. Almost 25 percent of the satellite communications used commercial systems (Winnefield, 1994:205). In all, over ten different military and commercial communications satellite systems were used to support the Gulf War effort.

The development of the satellite communications network during Operation Desert Shield/Storm was a major achievement. Twenty-five major network reconfigurations were undertaken by the Air Force alone during the development of the satellite communications system.

Prior to Operation Desert Shield, there were three tactical satellite terminals and one shipboard terminal supporting CENTCOM in the theater. These terminals supported a data rate or throughput of 4.54 MBPS using strictly United States military satellite

assets. By 3 September 1990, the number of Defense Satellite Communications System (DSCS) tactical satellite terminals had increased to 48 and the total satellite throughput reached 38.27 MBPS. At this point in time, one of the two military satellites (Indian Ocean and East Atlantic) supporting this region of the world became saturated. Channel usage was reconfigured between the two satellites to optimize total throughput.

After satellite channel usage was maximized on 15 September 1990, total throughput was increased slightly to 38.59 MBPS but the number of DSCS terminals increased to 53. At this point, all of the theater satellite assets were saturated. It was decided to move a reserve satellite (Western Pacific Reserve) over the Pacific Ocean to a position over the CENTCOM area of responsibility. Also, the United Kingdom offered us 3.5 MBPS capacity on their SKYNET satellite. In developing an information campaign plan, all assets should be examined so contingency plans can be developed if necessary.

By 17 November 1990, it was decided to use commercial assets to alleviate our problem with saturation of military satellites. DSCS throughput dropped to 36.22 MBPS even through the number of tactical terminals increased to 54. There were two commercial terminals using INTELSAT passing a throughput of 12.35 MBPS. This shows the need for a campaign planner to be familiar with commercial satellite systems.

The Western Pacific Reserve Satellite was positioned over the theater but was not yet operational by 19 December 1990. By this time the number of DSCS satellite terminals had grown to 59 supporting a throughput of 41.34 MBPS. Our reliance on

commercial satellites continued to grow. At this point in time, there were six commercial terminals supporting a data throughput of 29.24 MBPS using INTELSAT. The Western Pacific Reserve Satellite was operational by 15 January 1991. This allowed us to support 110 DSCS terminals for a total throughput of 67.65 MBPS. Also, INTELSAT supported six terminals for a throughput of 30.82 MBPS. These statistics are summarized in the following figure: (Bedrosian and others, 1991:9)

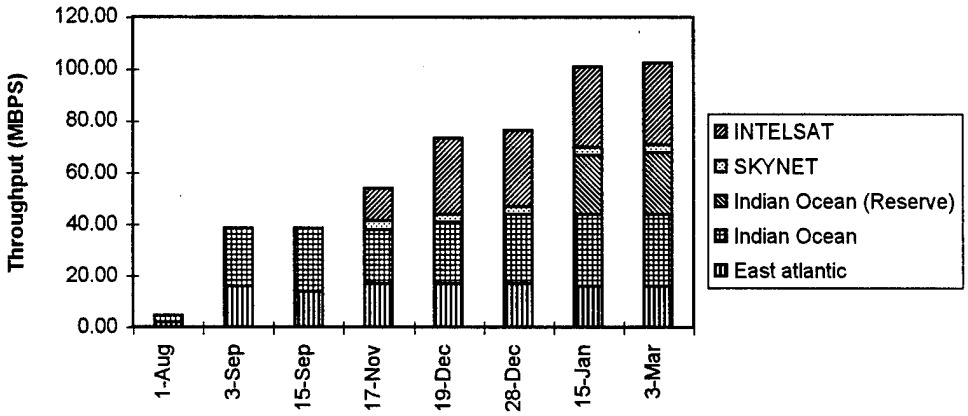

Figure 7. Buildup of CENTCOM Satellite Network

To accommodate for this projected but unpredictable growth, a hub-spoke configuration was used for satellite communications network development. The goal was to minimize network perturbations by anchoring communications through a central hub. Spokes could be added or relocated as necessary. The first hub was installed at Thumrait, Oman for two reasons: stability and safety. Thumrait was in the rear area out of SCUD range and in an area where our forces probably would not have to leave. Al

Dahfra, UAE became the second hub and finally in November 1990, Riyadh, Saudi Arabia was added as a hub. Each time a hub was added the satellite network had to be reengineered (McKenzie, 1991:6-1).

There were also a very large number of small UHF satellite terminals in theater. These terminals were located in the wing operations centers, tactical air control center, airlift control elements, and certain aircraft. They were used primarily for critical, time-sensitive command control information. One of the most critical functions the terminals supported was initial SCUD warnings. These terminals are very good for functions where the information is very low volume but extremely time-sensitive.

The Media. The media can be used to improve our acquisition of information. General Fogleman related the following personal experience during a speech at the Airlift/Tanker Association convention in 1993:

> I was in New Zealand when, on CNN, I saw the pictures of an American Serviceman's body being dragged through the streets in Mogadishu. It disappointed and incensed me as an American, so I spoke by conference call to the deputy commander-in-chief at TRANSCOM, to the vice-commander at AMC, and to the TACC commander. I made it very clear to them that I knew the tasking was coming, and that we were going to meet that tasking. I told them that I did not care what regulation, what guidance, or what publication had to be waived, we were going to get armor to those people in Mogadishu. (Fogleman, 1994:18)

This example shows how sometimes the media can get information to our military commanders faster than our military communications channels. This additional information can be used to enhance our overall effectiveness.

The media can place reporters in locations where our military forces may not have access, such as Baghdad during Desert Storm. These reporters may be able to provide real time feedback on how the conflict is progressing or some intelligence information.

On the night the Gulf War started, a senior officer in the Pentagon Command Center, watching the television transmissions from Baghdad, checked his watch and consulted those planning the attack on the Iraqi central telecommunications tower: "if the cruise missile is on target . . . the reporter will go off the air right about (he counts down the seconds) . . . now" (Stech, 1994:234) The ABC and NBC reports, which were routed through the telecommunications tower, went dead. Our military leaders had instantaneous feedback that the attack on that target, at least in the short term, had been effective.

Real time reporting from behind the enemy lines can also provide us with real-time intelligence. The weather conditions at that enemy's location can be observed. In the case of the Gulf War, the locations and possibly the type of anti-aircraft artillery could be derived from watching the live reports from Baghdad. However, our forces need to be careful that the enemy is not using deception. Decoys could be set up around the reporter or actual forces may be hidden.

The Infosphere. An information campaign planner should also be familiar with the concept of the infosphere. The Directorate of Command, Control, Communications and Computer Systems of the Joint Staff (J6) published C4I for the Warrior in 1993 to establish joint interoperability for our forces. This document has the vision of providing

a warrior a fused, real-time true representation of the battlespace at any time and place. The infosphere will be the medium through which this representation is transmitted and is defined as "a global network of military and commercial communications systems and networks linking information databases and fusion centers that are accessible to the warrior anywhere, anytime, in the performance of any mission" (The Joint Staff, 1993:10).

Quality information needs to be provided to the user through the infosphere. Joint Pub 6-0: Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations lists seven criteria that determine the quality of information. These criteria are shown in the Figure 8 (JCS, 1995a:I-5).

ACCURACY
Information that conveys the true situation.

RELEVANCE
Information that applies to the mission, task, or situation at hand.

TIMELINESS
Information that is available in time to make decisions.

USABILITY
Information that is in common, easily understood format and displays.

COMPLETENESS
All necessary information required by the decisionmaker.

BREVITY
Information that has only the level of detail required.

SECURITY
Information that has been afforded adequate protection where required.

Figure 8. Information Quality Criteria

If information is of sufficient quality, it will aid in achieving the objective of enhancing overall effectiveness. Basically, the users should be provided what they want, where they want it, when they want it, and in the form they want it.

IV. Conclusions

Introduction

This chapter will identify some of the considerations that need to be taken into account in the development of an information warfare campaign plan. These considerations will be consolidated from the information presented in Chapters II and III. These considerations will give future planners a starting point for developing information campaign plans.

Joint Effort

Since U.S. warfare is joint, the information campaign plan needs to support the combatant commander's joint campaign plan. This plan needs to support the combatant commander's objectives and concepts of operation. The information operations in the campaign plan need to be synchronized with air, land, sea, space, and special operations in time, space, and effort. Furthermore, the Air Force's information warfare plan needs to support the overall information warfare effort. If information campaign plans are developed within this framework, they will assist in unifying the focus for our conduct of warfare.

Fundamentals of Campaign Plans

Many information planners will be developing campaign plans for the very first time. A planner should consider the fundamentals of campaign plans listed in Chapter II

of this paper. These fundamentals will give the planner a good set of guidelines for the development of an information campaign plan. Although a few of these fundamentals may not apply to the current planning situation, the majority will. Therefore, a campaign planner should look at each of the twelve fundamentals, determine the applicability, and incorporate those applicable fundamentals into the information campaign plan.

Centers of Gravity

Two of the fundamentals of campaign plans relate to centers of gravity and are of great importance to an information planner. The first objective is to identify and provide guidance for defeating enemy strategic and operational centers of gravity. The second objective is to identify and provide guidance for protecting friendly centers of gravity.

The five rings model can be used to identify centers of gravity. A list of typical strategic and operational centers of gravity was developed in Table 1. These centers of gravity exist for both friendly and enemy forces. Once these centers of gravity have been identified, the campaign planner should develop guidance for defeating the enemy's and protecting friendly centers of gravity.

Satellite Communications

Our military forces are becoming increasingly dependent on the flow of information. Satellites provide the means to transmit a large amount of information in a timely manner. Information campaign planners need to be aware of all satellite communications systems, military and commercial, at their disposal. A campaign

planner also needs to be prepared to operate if the satellites are jammed. Plans should be prepared to handle the loss of communications capacity under conditions of jamming.

Communications Network Survivability

An information campaign planner needs to design communications networks that are as invulnerable to attack as possible. As a minimum, the planner should not develop networks that are separable, meaning the destruction of one site or link will disrupt the network. Hopefully, these networks will be designed so that the node and edge connectivity will be as close as possible to $\lfloor 2e/n \rfloor$.

Satisfying Information Warfare Objectives

The information campaign plan should seek to satisfy the objectives of information warfare. In Chapter III, the new Air Force roles and missions for information warfare were discussed. Counter information, both offensive and defensive, C2 attack, and information operations should be used to obtain information superiority just as air roles and missions are used to achieve air superiority.

This paper analyzed how information missions can be used to obtain the information warfare objectives in the Cornerstones of Information Warfare. It is to be hoped that actual information campaign objectives will not be as broad. A similar analysis can be performed by the information campaign planner to achieve the more focused objectives spelled out in the supported commanders campaign plan.

Plan for the Media

The media has great information gathering capabilities. They have large numbers of people worldwide; many of which are in locations our military forces do not have access to. In wartime, there may actually be reporters in the enemy's territory providing live broadcasts. Future information planners should investigate the possibility of deploying with equipment capable of receiving CNN broadcasts. These broadcasts could be used to provide real time information on political events or be of some intelligence value.

Giving the Users What They Want

During the development of campaign plans for information warfare, planners need to be in contact with the information users. This information needs to be what the users wants, when they want it, and in the required format. The campaign planner needs to work with the various users to get firm information requirements. Whenever possible, the required information should be able to be pulled by the user versus being pushed. This will result in less information for the user compressing the OODA loop.

Information planners need to provide users with quality information. Planners should analyze the information being provided for accuracy, relevance, timeliness, usability, completeness, brevity, and security. If all these quality criteria can be met, our military forces will be much more effective.

Summary

While there has been much written about information warfare, little of the literature is related to planning. In this chapter, a list of considerations for information warfare campaign plans was presented. These considerations were discussed from the view point of developing a campaign plan. This list, while not all inclusive, will hopefully provide future information warfare planners a foundation for developing campaign plans.

Bibliography

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" Cooperative Strategy, 12: 141-165 (April-June 1993).

Bedrosian, E., and others. Tactical Satellite Orbital Simulation and Requirements Study. Contract MDA903-91-C-0006. Santa Monica CA: RAND, 1993 (N-3568-A).

Campen, Alan. The First Information War: The Story of Communication, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax VA: Armed Forces Communications and Electronics Association International Press, 1992.

Cohen, Eliot A. Gulf War Air Power Survey: Volume IV - Weapons, Tactics and Training and Space Operations. Washington DC: GPO, 1993.

Deo, Narsingh. Graph Theory with Applications to Engineering and Computer Science. Englewood Cliffs NJ, 1974.

Department of the Air Force. Cornerstones of Information Warfare. USAF Concept Paper. Washington DC: HQ USAF, 11 August 1995.

-----. "Information Warfare," Air Force Doctrine Document (AFDD) 5, Preliminary Draft, 1995.

Fadok, Major David S. John Boyd and John Warden: Air Power's Quest for Strategic Paralysis. Maxwell AFB AL: Air University Press, February 1995 (AD-A291621).

Fogleman, General Ronald R., "The Fifth Dimension of Warfare." Remarks as delivered to Armed Forces Communications and Electronics Association, Washington DC, 25 April 1995.

-----. "White Paper: Leadership for Changing Times," Airlift/Tanker Quarterly, 2: 18-23 (Winter 1994).

Haeni, Reto E. "An Introduction to Information Warfare." Term paper for Computer Security Systems I, George Washington University, Washington DC. 1995.

Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer, (C4) Systems Support to Joint Operations. Joint Pub 6-0. Washington DC: JCS, 30 May 1995.

-----. Doctrine for Joint Operations. Joint Pub 3-0. Washington DC: JCS, 1 February 1995.

-----. Doctrine for Joint Psychological Operations. Joint Pub 3-53. Washington DC: JCS, 30 July 1993.

-----. Doctrine for Planning Joint Operations. Joint Pub 5-0. Washington DC: JCS, 13 April 1995.

-----. Joint Doctrine for Military Deception. Joint Pub 3-58. Washington DC. JCS, 6 June 1994.

-----. Joint Warfare of the US Armed Forces. Joint Pub 1. Washington DC. JCS, 11 November 1991.

The Joint Staff, J-6. C4I for the Warrior. Washington DC: The Joint Staff, 12 June 1993.

Kaplan, Colonel Len. The Air Force Responds to a 21st Century World - Information Warfare. Briefing slides. HQ AF/SCXX, Washington DC, 1995.

Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington DC: National Defense University Press, 1994.

Magsig, Daniel E. "Information Warfare in the Information Age." George Washington University Washington DC. 1995

McKenzie, Dave. "Satellite Network Development," in Air Force Tactical Communications in War: The DESERT SHIELD/DESERT STORM Comm Story. Ed. Randy Witt. Riyadh Saudi Arabia: HQ United States Central Command Air Forces, March 1991.

Munro, Neil. "The Pentagon's New Nightmare: An Electronic Pearl Harbor," The Washington Post, 16 July 1995.

National Security Council. National Policy for the Security of National Security Telecommunications and Information Systems. National Security Decision Directive 145. Washington DC: GPO, 5 July 1990.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Schwenk, Charles R. The Essence of Strategic Decision Making. New York: Lexington Books, 1988.

Spellman, Marc I. "ECM and Satellite Communication Network Control," in Air and Satellite Communications. Ed. John L. McLucas. Washington DC: AFCEA International Press, 1985.

Stech, Frank J. "Preparing for More CNN Wars" in Essays on Strategy XII. Ed. John N. Petrie. Washington DC: National Defense University Press, 1994.

Szafranski, Colonel Richard. "A Theory of Information Warfare: Preparing for 2020," Airpower Journal, IX: 56-65 (Spring 1995).

Waller, Douglas. "Onward Cyber Soldiers," Time Magazine, 146: 21 August 1995.

Warden, John A. The Air Campaign: Planning for Combat. Washington DC: National Defense University Press, 1988.

Warden, Colonel John A. "The Enemy as a System," Airpower Journal, IX: 41-55 (Spring 1995).

Widnell, Sheila E. "Information Technology Vital to Battlefield Success" Remarks prepared for delivery at the Air Force Anniversary Ball sponsored by the Air Intelligence Agency, San Antonio TX, 22 September 1995.

Winnefield, James A. and others. A League of Airmen: U.S. Air Power in the Gulf War. Contract F49620-91-C-0003. Santa Monica CA. RAND, 1994 (MR-343-AF).

Vita

Capt Andrew H. Pears was born on 7 July 1961 in Meadville, Pennsylvania. He graduated from Meadville Area Senior High in 1979 and entered undergraduate studies at Clarion University of Pennsylvania. He graduated with a Bachelor of Science degree in Physics in May 1984. He received his commission on 17 December 1985 upon graduation from Officer Training School.

His first assignment was with Strategic Communications Division, Offutt AFB, Nebraska, where he served as a Plans and Exercises Staff Officer and later as Chief, Southwest Asia Plans and Exercises Branch. In July 1989, Capt Pears was assigned to the 4525th Combat Applications Squadron at Hanscom AFB, Massachusetts as Chief, Tactical C4I Systems Branch. While there, he deployed as Chief, Operations for the 61st Combat Communications Squadron (Provisional) at Riyadh Air Base, Saudi Arabia. In December 1992, he was assigned to the 436th Communications Squadron at Dover AFB, Delaware as Commander, Plans and Implementation Flight and later as Commander, Systems Flight.

In February 1995, Capt Pears was assigned to the Air Mobility Warfare Center as a Student, Advanced Study of Air Mobility. After graduation, he will be assigned to the Command, Control, Communications, and Computer Systems Directorate at United States Transportation Command.

Permanent Address: RD#3 Box 306
Meadville, PA 16335

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 1996	Graduate Research Paper

4. TITLE AND SUBTITLE

PLANNING FOR THE INFORMATION CAMPAIGN

5. FUNDING NUMBERS

6. AUTHOR(S)

Andrew H. Pears, Capt, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology,
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GMO/LAR/96J-8

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

HQ AMWC/WCOA
FT DIX NJ 08640

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Desert Storm demonstrated the importance of dominating the information realm during a conflict. Information warfare is the means through which our forces can maintain information dominance on future battlefields. Air Force doctrine is currently being modified to include three new roles and missions related specifically to information warfare. Plans for future conflicts should include these new roles and missions. Campaign plans serve as the unifying focus for our conduct of warfare. This study examines the various aspects of campaign planning and information warfare. This research provides future planners eight specific information campaign planning recommendations. It is recommended that the information campaign plan support the joint effort, follow the fundamentals of campaign plans (JCS Pub 5-0), and accomplish information warfare objectives. Furthermore, information campaign planners should examine communications network survivability, friendly and enemy centers of gravity, satellite systems capabilities and vulnerabilities, the possible effects of the media, and specific user requirements.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Warfare, Military Planning, Campaigns Center of Gravity, Command Control Communications	65
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

AFIT Control Number AFIT/GMO/LAR/96J-8

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to determine the potential for current and future applications of AFIT research. **Please return completed questionnaire** to: DEPARTMENT OF THE AIR FORCE, AFIT/LAC BLDG 641, 2950 P STREET, WRIGHT-PATTERSON AFB OH 45433-7765 or e-mail to dvaughan@afit.af.mil or nwiviott@afit.af.mil. Your response is **important.** Thank you.

1. Did this research contribute to a current research project? a. Yes b. No

2. If you answered YES to Question #1, do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not researched it? a. Yes b. No

3. The benefits of AFIT research can often be expressed by the equivalent value that your agency received by virtue of AFIT's performing the research. **Please estimate** what this research would have cost in terms of manpower and dollars if it had been accomplished under contract or if it had been done in-house.

Man Years_____ $_____

4. Whether or not you were able to establish an equivalent value for this research (in Question 3), what is your estimate of its significance?

a. Highly Significant b. Significant c. Slightly Significant d. Of No Significance

5. Comments (Please feel free to use a separate sheet for more detailed answers and include it with this form):

_____ _____

Name and Grade Organization

_____ _____

Position or Title Address